CLAIMS

What is claimed is:

1. A method for managing access to data in a database subject to a plurality of label-based security policies, the method comprising the steps of:

receiving, within a database management system, a request for performing an operation set of one or more operations on data in a table of the database;

determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and

for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set.

2. A method according to Claim 1, further comprising adding a policy column to the table for each policy in the policy set associated with the table

3. A method according to Claim 2, further comprising storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

4. A method according to Claim 2, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

5. A method according to Claim 1, wherein the policy set associated with the table includes two or more policies of the plurality of label-based policies.

Sub A1

6. A method for managing access to data in a database based on a database policy set of one or more label-based security policies, the method comprising the steps of:

registering, with a database management system, one or more package of routines, wherein each package implements a security model that supports a model set of one or more policies of the database policy set and each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

7. A method according to Claim 6, further comprising the step of forming each package so that the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

8. A method according to Claim 7, said step of forming the package further comprising including one or more administrative routines for defining a policy for the model set.

9. A method according to Claim 8, said step of including one or more administrative routines for defining a policy further comprising including one or more administrative routines for defining a name for a particular policy; labels for the particular policy; descriptions for the labels; and properties for the labels.

10. A method according to Claim 6, further comprising the step of invoking an administrative routine of the first package for defining the first policy.

Page 34 of 50 pages

11. A method according to Claim 10, said step invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

12. A method according to Claim 6, further comprising, in response to attempts to operate on data in a row in the table, the step of determining that the first policy applies to the table.

13. A method according to Claim 6, further comprising the steps of:

associating a second policy of a second model set in a second package with a second table within the database system; and

invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

14. A method according to Claim 13, wherein the second model in the second package is the same as the first model in the first package.

15. A method according to Claim 13, wherein the second model in the second package is different from the first model in the first package.

16. A method according to Claim 13, wherein the second table is the same as the first table.

17. A method according to Claim 13, wherein the second table is different from the first table.

18. A method according to Claim 6, said step of invoking the access mediation routine in the first package further comprising providing data indicating the first policy to the access mediation routine.

19. A method according to Claim 6, wherein.

the method further comprises the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included the set of allowed labels for the first policy.

20. A method according to Claim 19, further comprising the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user.

21. A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database subject to a plurality of label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving a request for performing an operation set of one or more operations on data in a table of the database;

determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and

for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set of labels corresponding to the policy set.

22. A computer-readable medium according to Claim 21, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of adding a policy column to the table for each policy in the policy set associated with the table

23. A computer-readable medium according to Claim 22, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

24. A computer-readable medium according to Claim 22, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

25. A computer-readable medium according to Claim 21, wherein the policy set associated with the table includes two or more policies of the plurality of label-based policies.

Sub A4

26. A computer-readable medium carrying one or more sequences of instructions for managing access to data in a database based on a database policy set of one or more label-based security policies, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

registering, with a database management system, one or more package of routines, wherein each package implements a security model that supports a model set of one or more policies of the database policy set and each package includes an access mediation routine;

associating a first policy of a first model set in a first package with a first table within the database system; and

invoking the access mediation routine in the first package for determining whether to allow operation on data in the first table based on the first policy.

27. A computer-readable medium according to Claim 26, wherein the access mediation routine conforms to a specified interface for enforcing a policy in the database management system.

Sub A5

28. A computer-readable medium according to Claim 27, wherein the package includes one or more administrative routines for defining a policy for the model set.

29. A computer-readable medium according to Claim 28, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of defining a name for a particular policy; labels for the particular policy; descriptions for the labels; and properties for the labels.

30. A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of invoking an administrative routine of the first package for defining the first policy.

31. A computer-readable medium according to Claim 30, said step invoking the administrative routine of the first package further comprising providing to the administrative routine of the first package a plurality of parameters including a policy name for the first policy and a plurality of label names for labels of the first policy.

32. A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform, in response to attempts to operate on data in a row in the table, the step of determining that the first policy applies to the table.

33. A computer-readable medium according to Claim 26, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the steps of:

associating a second policy of a second model set in a second package with a second table within the database system; and

invoking the access mediation routine in the second package for determining whether to allow operation on data in the second table based on the second policy.

34. A computer-readable medium according to Claim 33, wherein the second model in the second package is the same as the first model in the first package.

35. A computer-readable medium according to Claim 33, wherein the second model in the second package is different from the first model in the first package.

36. A computer-readable medium according to Claim 33, wherein the second table is the same as the first table.

37. A computer-readable medium according to Claim 33, wherein the second table is different from the first table.

38. A computer-readable medium according to Claim 26, said step of invoking the access mediation routine in the first package further comprising providing data indicating the first policy to the access mediation routine.

39. A computer-readable medium according to Claim 26, wherein.

execution of the one or more sequences of instructions further causes the one or more processors to perform the step of determining a set of allowed labels for the first policy for a user of the database management system;

said step of invoking the access mediation routine is performed during said step of determining the set of allowed labels; and

the user is allowed to operate on the data according to the first policy if the data is associated with a label for the first policy and the label is included the set of allowed labels for the first policy.

40. A computer-readable medium according to Claim 39, wherein execution of the one or more sequences of instructions further causes the one or more processors to perform the step of storing the set of allowed labels in a session cache for a communication session between the database management system and the user.